

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON AT SEATTLE

STEVEN VANCE and TIM JANECYK, for
themselves and others similarly situated,

Plaintiffs,

No.

AMAZON.COM, INC.,

Defendant.

CLASS ACTION COMPLAINT

JURY DEMAND

CLASS ACTION COMPLAINT

Plaintiffs STEVEN VANCE and TIM JANECYK, on behalf of themselves and all other similarly situated individuals (“Plaintiffs”), by and through their respective attorneys, bring this Class Action Complaint against Defendant Amazon.com, Inc. (“Amazon”) and allege the following:

INTRODUCTION

1. Facial recognition technology – once a thing only seen in movies – now threatens to end individual privacy. Public and private entities increasingly deploy facial recognition products to determine a private citizens' identities, as well as other personal information, such as their addresses, phone numbers, whereabouts and acquaintances.

2. Unlike the way facial recognition technology is depicted in the movies, the actual technology is plagued by a major problem – it is inaccurate, especially when it comes to correctly identifying women and people of color.

3. In recent years, an “arms race” has developed amongst for-profit companies seeking to become market leaders in the facial recognition arena. Critical to winning this battle

has been to the ability to claim a low identification error rate – *i.e.*, the for-profit companies want to herald the accuracy of their products, including accuracy in identifying women and people of color.

4. In its effort to improve its facial recognition technology, Defendant Amazon violated Illinois' Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA"), by, among other things, unlawfully collecting, obtaining, storing, using, possessing and profiting from the biometric identifiers and information of Plaintiffs Vance and Janecyk and all other similarly situated Illinois residents and citizens (hereinafter, the "Class Members").

5. Plaintiffs bring this Class Action Complaint seeking: (a) statutory damages of \$5,000 per BIPA violation, or, alternatively, if Defendant Amazon acted negligently, \$1,000 per BIPA violation, along with attorneys' fees and costs; (b) disgorgement of Defendant's ill-gotten gains derived from the use of the unlawfully-acquired data; and (c) an injunction (i) barring Defendant from any further use of Illinois citizens' and residents' biometric identifiers and information; (ii) barring Defendant from continuing to collect, obtain, store, use, possess and profit from Plaintiffs' and Class Members' biometric identifiers and information; and (iii) requiring Defendant to delete and destroy Plaintiffs' and Class Members' biometric identifiers and information.

PARTIES

6. At relevant times, Plaintiff STEVEN VANCE was – and remains – an Illinois resident who lived in the Northern District of Illinois. Defendant Amazon collected, obtained, stored, used, possessed and profited from Plaintiff Vance’s biometric identifiers and information – namely, facial geometric scans of Plaintiff Vance.

7. At relevant times, Plaintiff TIM JANECYK was – and remains – an Illinois resident who lived in the Northern District of Illinois. Defendant Amazon collected, obtained, stored, used, possessed and profited from Plaintiff Janecyk’s biometric identifiers and information – namely, facial geometric scans of Plaintiff Janecyk.

8. Defendant Amazon is a Delaware corporation headquartered in Seattle, Washington.

JURISDICTION AND VENUE

9. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) (the “Class Action Fairness Act”) because sufficient diversity of citizenship exists between the parties in this action, the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, and there are 100 or more members of the Class. Because it is estimated that the Class will have thousands of members and Defendant Amazon’s intentional and reckless violations of BIPA are punishable by statutory damages of \$5,000 per violation, the amount in controversy is well in excess of \$5,000,000. This Court has supplemental jurisdiction over the state law claim pursuant to 28 U.S.C. § 1367.

10. This Court has personal jurisdiction over Defendant Amazon because Amazon is at home in the Western District of Washington. As alleged above, Amazon is headquartered in Seattle, Washington.

11. Venue is proper under 28 U.S.C. § 1391(b)(1) because Defendant Amazon resides in the Western District of Washington.

FACTUAL ALLEGATIONS

Biometric Identifiers

12. Every individual has unique features by which he or she can be identified using a set of standard quantitative measurements, commonly referred to as “biometric identifiers.”

13. For example, the shape of and distance between tiny ridges on each person's finger are unique, so measures of those features can be used to identify a specific individual as the person who made a fingerprint.

14. Each person also has a unique facial geometry composed of, among other measures, distances between key facial landmarks and ratios between those distances.

15. Once a picture of a person's face is scanned and its biometric measurements are captured, computers can store that information and use it to identify that individual any other time that person's face appears on the internet, in a scanned picture or footage from any of the billions of cameras that are constantly monitoring the public's daily lives.

16. Unlike fingerprints, however, facial biometrics are readily observable and, thus, present a grave and immediate danger to privacy, individual autonomy and liberty.

The Illinois Biometric Information Privacy Act

17. Through BIPA, Illinois strictly regulates the collection, obtainment, storage and use of biometric identifiers.

18. Under BIPA, biometric identifiers include a scan of an individual's face geometry. 740 ILCS § 14/10.

19. Under BIPA, biometric information is “any information . . . based on an individual’s biometric identifier used to identify an individual.” 740 ILCS § 14/10.

1 20. According to the Illinois General Assembly: “[b]iometrics are unlike other
 2 unique identifiers that are used to access finances or other sensitive information. For example,
 3 social security numbers, when compromised, can be changed. Biometrics, however, are
 4 biologically unique to the individual; therefore, once compromised, the individual has no
 5 recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-
 6 facilitated transactions.” 740 ILCS § 14/5(c).

8 21. Pursuant to BIPA, a private entity is, among other things: (a) prohibited from
 9 collecting or otherwise obtaining an individual’s biometric identifiers and information without
 10 providing written notice and obtaining a written release; (b) prohibited from profiting from an
 11 individual’s biometric identifiers and information; and (c) required, to the extent it is in
 12 possession of biometric identifiers or information, to develop a written policy, made available to
 13 the public, that establishes a retention schedule and guidelines for permanently destroying such
 14 identifiers and information. 740 ILCS § 14/15.

15 22. BIPA provides for a private right of action and allows a prevailing party to
 16 recover liquidated damages in the amount of: (a) \$1,000 or actual damages, whichever is
 17 greater, for negligent violations of its provisions; and (b) \$5,000 or actual damages, whichever
 18 is greater, for intentional or reckless violations of its provisions. 740 ILCS § 14/20. BIPA also
 19 allows for the recovery of attorneys’ fees and costs and injunctive relief. 740 ILCS § 14/20.

23 ***Facial Recognition Technology***

24 23. Facial recognition is a form of computer artificial intelligence the goal of which
 25 is to “create systems that detect, recognize, verify and understand characteristics of human
 26 faces.”¹

27
 28 ¹ Michele Merler, *et al.*, *Diversity in Faces*, IBM Research AI (Apr. 10, 2019) (“*Diversity in Faces*”).
 CLASS ACTION COMPLAINT - 5

1 24. To do this well, the algorithms driving facial recognition technology must be
 2 trained with and fed vast quantities of images of a diverse array of faces. To satisfy the ever-
 3 growing demand for myriad high-resolution images of faces, unchecked companies have begun
 4 turning to the internet, where photographs are sometimes taken without the photographer's or
 5 subject's knowledge or consent. This has been called the dirty little secret of AI training sets.
 6 Researchers often just grab whatever images they can find "in the wild."

7 25. Facial recognition products rely on machine learning algorithms that are trained
 8 with labeled data.² As a result, algorithms trained with biased data can result in algorithmic
 9 discrimination,³ which, in turn, can lead to facial recognition products that are less effective at
 10 identifying certain types of faces.

11 26. For example, an algorithm trained on a dataset that underrepresents a group or
 12 subgroup – e.g., woman or people of color – will have a higher rate of error with respect to
 13 identifying members of those groups or subgroups.

14 27. Historically, available datasets on which facial recognition algorithms were
 15 trained contained a disproportionate number of light-skinned males.

16 **Flickr**

17 28. At relevant times, Flickr was a photo-sharing website that had access to over 100
 18 million photographs posted by Flickr users.

19 29. In or about 2014, Flickr – through its parent company Yahoo! – compiled
 20 approximately 100 million Flickr photographs into a single dataset (the "Flickr Dataset") and
 21 made the dataset publicly available.

22
 23 ² Joy Buolamwini, et al., *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender*
 24 *Classification, Proceedings of Machine Learning Research* 81:1-15 (2018) at 1.

25 ³ *Id.*

1 30. Flickr did so without informing or receiving the consent of the individuals who
 2 uploaded these photographs to Flickr or who appeared in these photographs.

3 31. Flickr contended that its purpose in releasing the Flickr Dataset was to help
 4 improve the accuracy and reliability of facial recognition technology.
 5

6 32. The Flickr Dataset contained images of Illinois citizens and residents, including
 7 images of Plaintiffs and Class Members.

8 ***The Gender Shades Study***

9 33. In or about February 2018, researchers released *Gender Shades: Intersectional*
 10 *Accuracy Disparities in Commercial Gender Classification* (“*Gender Shades*”) in which they
 11 noted that prior studies had shown that “machine learning algorithms can discriminate based on
 12 classes like race and gender.”⁴

14 34. Building on that prior research, the researchers analyzed three commercial facial
 15 recognition products focusing on each product’s ability to accurately identify gender.⁵

16 35. The study determined that each product more accurately classified: (a) males
 17 than females; and (b) lighter individuals than darker individuals.⁶

19 36. Significantly, the error rate with respect to accurately classifying darker females
 20 was 20.8% for Defendant Amazon, specifically, and as high as approximately 34.7%.⁷

21 37. The researchers concluded that the “most improvement is needed on darker
 22 females specifically. More broadly, the error gaps between male and female classification along
 23 with lighter and darker classification should be closed.”⁸

25
 26 ⁴ *Id.*

27 ⁵ *See id.* at 8.

28 ⁶ *Id.*

⁷ *Id.* at 9.

⁸ *Id.* at 11.

1 38. In a follow-up to *Gender Shades*, the researchers examined the accuracy of
 2 Defendant Amazon's Rekognition facial recognition technology, as compared to the
 3 technologies examined in the original study and as modified after the study.⁹
 4

5 39. The updated study found that Rekognition had an error rate of 31.37% with
 6 respect to identifying dark-skinned females, as opposed to an error rate of 0.00% with respect to
 7 identifying light-skinned males.¹⁰

8 ***Response to Gender Shades***

9 40. In the aftermath of *Gender Shades*, companies felt pressured to improve the
 10 accuracy of, and reduce the bias in, their facial recognition products.

12 41. In or about April 2019, International Business Machines Corporation ("IBM")
 13 noted that a "critical aspect limiting face recognition performance in practice is facial diversity,"
 14 begging the question "does the training data for [face recognition] systems fairly represent the
 15 distribution of faces we see in the world?"¹¹

17 42. To respond to the issue, IBM created Diversity in Faces – a new dataset
 18 consisting of one million images culled from the Flickr Dataset – for the purpose of improving
 19 the ability of facial recognition systems to fairly and accurately identify all individuals (the
 20 "Diversity in Faces Dataset").¹²

21 43. In creating the Diversity in Faces Dataset, IBM scanned the facial geometry of
 22 each image contained in the dataset and created a "comprehensive set of annotations of intrinsic
 23 facial features that includes craniofacial distances, areas and ratios, facial symmetry and

25 ⁹ Inioluwa Deborah Raji, et al., *Actionable Auditing: Investigating the Impact of Publicly Naming Biased*

26 Performance Results of Commercial AI Products, Ass'n for the Advancement of Artificial Intelligence
 27 (2019).

28 ¹⁰ *Id.* at 4.

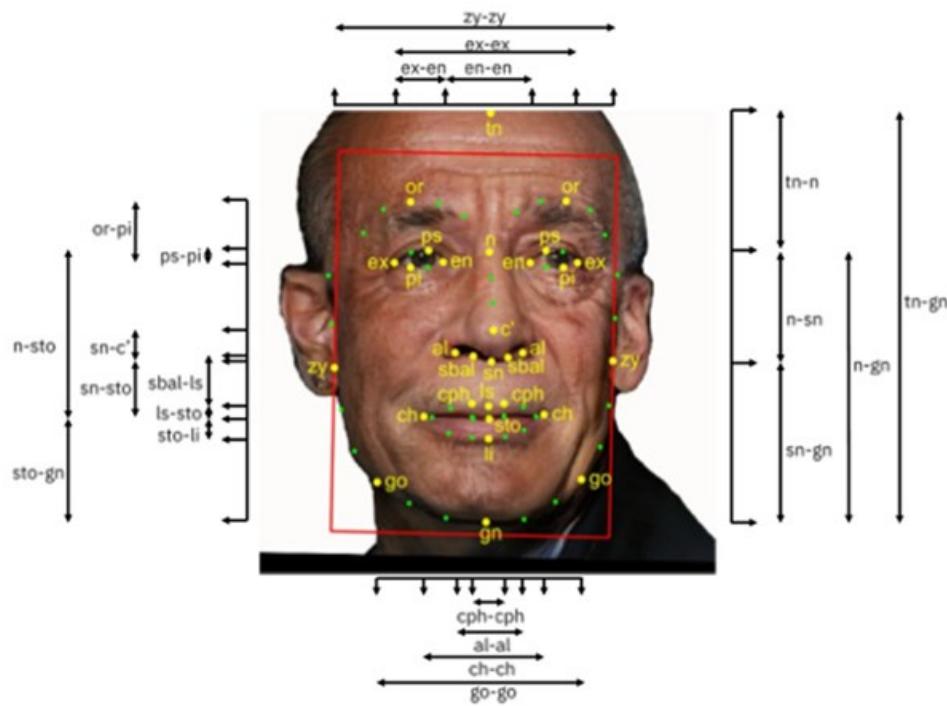
¹¹ *Diversity in Faces*, *supra*, at 1.

¹² *See id.*

1 contrast, skin color, age and gender predictions, subjective annotations, and pose and
 2 resolution.”¹³

3 44. To build the Diversity in Faces Database, IBM extracted 19 facial landmark
 4 points from each image in the dataset to determine 68 key points for each face.¹⁴
 5

6 45. IBM used the 19 facial landmark points to extract craniofacial features for each
 7 image, as shown in the figure below¹⁵:



21 46. The Diversity in Faces Dataset contained the biometric identifiers and
 22 information of Plaintiffs and Class Members.

24 47. IBM did not seek nor receive permission from Plaintiffs or Class Members to
 25 include their images in the Diversity in Faces Dataset, let alone to perform scans of their facial
 26

27 ¹³ *Id.* at 2.

28 ¹⁴ *Id.* at 9.

15 *Id.* at 9-10.

1 geometries or to otherwise collect, obtain, store, use, possess or profit from their biometric
 2 identifiers and information.

3 48. In or about April 2019, IBM published a journal article describing the Diversity
 4 in Faces Dataset in great detail and making clear that the dataset contained the biometric
 5 identifiers and information of each individual who appeared in the dataset.

6 49. IBM made the Diversity in Faces Dataset available to other for-profit companies
 7 that developed, produced, marketed, sold or otherwise used facial recognition products and
 8 technologies in connection with their for-profit businesses.¹⁶

9 50. To obtain the Diversity in Faces Dataset from IBM, a company had to apply for
 10 permission from IBM via an online questionnaire.

11 51. If IBM granted access to the Diversity in Faces Dataset, the company seeking
 12 access had to download the dataset from a link provided by IBM.

13 52. The information provided to companies that downloaded the Diversity in Faces
 14 Dataset included the biometric identifiers and information extracted from each photograph in
 15 the dataset and links to each photograph on Flickr from which IBM extracted the biometric data.

16 53. From the Flickr links IBM provided to companies that downloaded the Diversity
 17 in Faces Dataset, the companies were able to identify the Flickr user who uploaded the
 18 photograph to Flickr, view the Flickr user's homepage and other posted material, and view each
 19 photograph's metadata, including any available geo-tags relating to where the photograph was
 20 taken or uploaded.

21
 22
 23
 24
 25
 26
 27
 28 ¹⁶ See *Diversity in Faces*, *supra*.
 CLASS ACTION COMPLAINT - 10

1 ***Defendant Amazon Obtained the Diversity in Faces Dataset***

2 54. At relevant times, Defendant Amazon developed, produced, marketed and
 3 otherwise used facial recognition products and technologies in connection with its business.
 4

5 55. Amazon's core facial recognition product is Amazon Rekognition, which
 6 (among other features) allows users to match new images of faces with existing, known facial
 7 images "based on their visual geometry, including the relationship between the eyes, nose,
 8 brow, mouth, and other facial features."¹⁷

9 56. On information and belief, Amazon Rekognition, is a fundamental cornerstone of
 10 many of Amazon's largest consumer products and services around the world, including but not
 11 limited to: (a) Amazon's photo platform – Amazon Photos; (b) Amazon's smart home systems
 12 and cameras, including the Ring video doorbell; and (c) Alexa, Amazon's virtual assistant
 13 technology that is integrated into mobile phone applications on Android and Apple operating
 14 systems. On information and belief, Amazon has also profited from selling its facial recognition
 15 technology to third parties.

16 57. Amazon is the largest provider of facial recognition technology to law
 17 enforcement agencies, and has marketed their Rekognition software to agencies such as ICE and
 18 the FBI, to monitor individuals they consider "people of interest."¹⁸ Amazon has also partnered
 19 with more than 1,300 law enforcement agencies, allowing them to use footage from their Ring
 20 home security cameras in criminal investigations.¹⁹ Amazon has expanded these efforts,

21
 22
 23
 24
 25

¹⁷ Amazon, *The Facts on Facial Recognition with Artificial Intelligence*,
 26 <https://aws.amazon.com/rekognition/the-facts-on-facial-recognition-with-artificial-intelligence/> (last
 27 accessed June 16, 2020)

28 ¹⁸ Karen Hao, *The two-year fight to stop Amazon from selling face recognition to the police*, MIT Tech.
Rev. (June 12, 2020), <https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/> (last visited June 22, 2020).

29 ¹⁹ *Id.*

1 marketing their facial recognition software to government agencies despite warnings from
 2 consumers, employees, members of Congress and shareholders.²⁰

3 58. In July 2018, the American Civil Liberties Union of Northern California
 4 (“ACLU”) published the results of a study of Rekognition’s accuracy.²¹

5 59. According to the ACLU’s study, Rekognition incorrectly matched 28 members
 6 of the United States Congress as people who had been arrested for a crime.²²

7 60. According to the study, the false matches disproportionately involved people of
 8 color.

9 61. After IBM made the Diversity in Faces Dataset available, Defendant Amazon
 10 applied for and obtained the Diversity in Faces Dataset from IBM.

11 62. Defendant Amazon obtained the Diversity in Faces Dataset in order to improve
 12 the fairness and accuracy of its facial recognition products and technologies.

13 63. On information and belief, upon obtaining the Diversity in Faces Dataset from
 14 IBM, Defendant Amazon used the links provided by IBM to download, copy or otherwise
 15 obtain from Flickr each photograph in the dataset, including Plaintiffs’ photographs, in order to
 16 associate the biometric identifiers and information provided by IBM with the actual
 17 photographs to which the biometric data related.

21 22²⁰ See Kate Conger, *Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts with Law Enforcement*, Gizmodo (June 21, 2018), <https://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognition-1827037509> (last accessed June 22, 2020); *Pressure Mounts on Amazon, Microsoft, and Google Against Selling Facial Recognition to Government*, ACLU Northern California (Jan. 15, 2019), <https://www.aclunc.org/news/pressure-mounts-amazon-microsoft-and-google-against-selling-facial-recognition-government> (last visited June 22, 2020); Heather Kelly, *Jeff Bezos: Amazon will keep working with the DoD*, CNN Business (Oct. 15, 2018), <https://www.cnn.com/2018/10/15/tech/jeff-bezos-wired/index.html> (last visited June 22, 2020).

22 23²¹ Jacob Snow, *Amazon’s Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU.org (July 26, 2018), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28> (last accessed June 18, 2020).

24 25²² *Id.*

1 64. Defendant Amazon obtained the Diversity in Faces Dataset in order to improve
 2 the fairness and accuracy of its facial recognition products and technologies.

3 65. Defendant Amazon profited from the biometric identifiers and information
 4 contained in the Diversity in Faces Dataset because those biometric identifiers and information
 5 allowed Amazon to improve its facial recognition products and technologies, including, upon
 6 information and belief, by allowing Amazon to improve the effectiveness of its facial
 7 recognition technology on a diverse array of faces, thereby making those products and
 8 technologies more valuable in the commercial marketplace.

9
 10 ***Allegations Related to Plaintiffs***

11 ***Plaintiff Vance***

12 66. In or about 2008, Plaintiff Vance uploaded to Flickr from his computer in Illinois
 13 a photograph of himself and two family members (the “2008 Photo”).

14 67. In addition to the 2008 Photo, Plaintiff Vance uploaded numerous other
 15 photographs to Flickr.

16 68. At relevant times, Plaintiff Vance’s publicly-accessible Flickr profile page
 17 clearly identified his Chicago, Illinois residence and provided a method for those accessing his
 18 page to contact him directly via Flickr’s internal “FlickrMail” direct message system, which
 19 Defendant Amazon chose not to do.

20 69. The 2008 Photo, as well as numerous other photographs uploaded to Flickr by
 21 Plaintiff Vance, are included in the Diversity in Faces Dataset obtained by Defendant Amazon.

22 70. Based on the links Defendant Amazon received from IBM, at relevant times, it
 23 knew that each of Plaintiff Vance’s photographs in the Diversity in Faces Dataset – including
 24 the 2008 Photo – originated from, and was affiliated with, his Flickr account.

71. Defendant Amazon never advised or informed Plaintiff Vance or his legal authorized representative in writing: (a) that it collected, stored and used Plaintiff Vance's biometric identifiers and information; or (b) of the specific purpose and length of term for which Plaintiff Vance's biometric identifiers and information were being collected, stored and used.

72. Defendant Amazon never received a written release executed by Plaintiff Vance or his legally authorized representative to collect, capture, receive, obtain, store or use his biometric identifiers and information.

73. As alleged in more detail below, Defendant Amazon's conduct has injured Plaintiff Vance and subjected him to additional imminent and certainly impending injuries.

Allegations Related to Plaintiff Janecyk

74. Plaintiff Janecyk is an accomplished photographer, having focused his work in portraiture and street life photography.

75. In 2008, Plaintiff Janecyk signed up for a Flickr account in the Village of Tinley Park, Illinois, and has since then uploaded in excess of a thousand of his photographs to Flickr. Among those photographs is a 2011 photograph depicting Plaintiff Janecyk's own face (the "2011 Photo"), which Plaintiff Janecyk uploaded to Flickr from his device in Illinois.

76. At relevant times, Plaintiff Janecyk's publicly-accessible Flickr profile page clearly identified his Illinois residence and provided a method for those accessing his page to contact him directly via Flickr's internal "FlickrMail" direct message system, which Defendant Amazon chose not to do.

77. The 2011 Photo, as well as numerous other photographs uploaded to Flickr by Plaintiff Janecyk, are included in the Diversity in Faces Dataset obtained by Defendant Amazon.

1 78. Based on the links Defendant Amazon received from IBM, at relevant times, it
 2 knew that each of Plaintiff Janecyk's photographs in the Diversity in Faces Dataset – including
 3 the 2011 Photo – originated from, and was affiliated with, his Flickr account.
 4

5 79. Defendant Amazon never advised or informed Plaintiff Janecyk or his legal
 6 authorized representative in writing: (a) that it collected, stored and used Plaintiff Janecyk's
 7 biometric identifiers and information; or (b) of the specific purpose and length of term for
 8 which Plaintiff Janecyk's biometric identifiers and information were being collected, stored and
 9 used.
 10

11 80. Defendant Amazon never received a written release executed by Plaintiff
 12 Janecyk or his legally authorized representative to collect, capture, receive, obtain, store or use
 13 his biometric identifiers and information.
 14

15 81. As alleged in more detail below, Defendant Amazon's conduct has injured
 16 Plaintiff Janecyk and subjected him to additional imminent and certainly impending injuries.
 17

Plaintiffs' and Class Members' Injuries and Damages

18 82. As a result of Defendant Amazon's unlawful conduct, Plaintiffs and Class
 19 Members have already sustained injuries and face many more imminent and certainly
 20 impending injuries, which injuries they will continue to suffer.
 21

22 83. Defendant Amazon chose to use and profit from biometric identifiers and
 23 information scanned from photographs that were uploaded from Illinois; managed via Illinois-
 24 based user accounts, computers and mobile devices; and/or created in Illinois. In so doing,
 25 Amazon exposed Illinois residents and citizens to ongoing privacy risks within Illinois,
 26 knowing that its conduct would injure those residents and citizens within Illinois. Further,
 27 Amazon knew or had reason to know that obtaining Illinois residents' and citizens' biometric
 28

1 identifiers and information in violation of BIPA would deprive those residents and citizens of
 2 their statutorily-protected privacy rights, neutralize Illinois residents' and citizens' abilities to
 3 control access to their biometric identifiers and information via their Illinois-managed devices,
 4 expose Illinois residents and citizens to potential surveillance and other privacy harms as they
 5 went about their lives within the state, and deter Plaintiffs and Class Members from publicly
 6 posting photographs. As such, Illinois had and has a direct interest in regulating the unlawful
 7 conduct alleged herein in order to protect the rights and interests of its residents and citizens.
 8

9 84. As the Illinois General Assembly has found and the Illinois Supreme Court has
 10 confirmed, the harm to Plaintiffs and Class Members as a result of Defendant Amazon's
 11 unlawful conduct has already occurred.

13 85. Further, as businesses worldwide compete to develop ever more advanced facial
 14 recognition technology, the race for data imperils the privacy of individuals everywhere,
 15 including the privacy of Plaintiffs and Class Members. Public policy in Illinois provides that
 16 given the risks of unwanted data collection and disclosure, its citizens need the power to make
 17 decisions about the fate of their unique biometric identifiers and information. Defendant
 18 Amazon's actions robbed Plaintiffs and Class Members of that power.

20 86. Moreover, as a result of Defendant Amazon's unlawful conduct, Plaintiffs' and
 21 Class Members' biometric identifiers and information are no longer under their control and are
 22 available to a potentially unlimited range of unknown individuals for whatever uses they please.
 23 These injuries, which are imminent and clearly impending, are in addition to the injuries
 24 Plaintiffs and Class Members have already sustained as a result of Defendant's actions.

26 87. As a result of Defendant Amazon's misconduct, Plaintiffs and Class Members
 27 have no recourse for the fact that their biologically unique information has been compromised.
 28

88. Moreover, as a result of Defendant Amazon's misconduct, Plaintiffs and Class Members are likely to withdraw from biometric-facilitated transactions and other facially-mediated electronic participation.

CLASS ACTION ALLEGATIONS

89. Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rule of Civil Procedure 23, seeking damages and equitable relief on behalf of the following Class for which Plaintiffs seek certification: All Illinois residents whose faces appear in the Diversity in Faces Dataset obtained by Defendant Amazon.

90. Excluded from the Class are: (a) Defendant Amazon; (b) any parent, affiliate or subsidiary of Defendant Amazon; (c) any entity in which Defendant Amazon has a controlling interest; (d) any of Defendant Amazon's officers or directors; or (e) any successor or assign of Defendant Amazon. Also excluded are any judge or court personnel assigned to this case and members of their immediate families.

91. Plaintiffs reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

92. **Numerosity.** While the exact number of Class Members is not known at this time, Defendant Amazon obtained the biometric identifiers and information from approximately one million images of faces, and Plaintiffs estimate the total number of Class Members to be in the thousands. Consistent with Rule 23(a)(1), the proposed Class is therefore so numerous that joinder of all members is impracticable. Class Members may be identified through objective means, including objective data available to Defendant Amazon regarding the images in the Diversity in Faces Dataset. Class Members may be notified of the pendency of this action by

1 recognized, Court-approved notice dissemination methods, which may include U.S. mail,
2 electronic mail, internet postings, social media and/or published notice
3

4 **93. Commonality and predominance.** Common questions of law and fact exist as
5 to all Class Members. These common questions of law or fact predominate over any questions
6 affecting only individual members of the proposed Class. Common questions include, but are
7 not limited to, the following:

- 8 a. Whether Defendant Amazon obtained the biometric identifiers and
9 information of Plaintiffs and Class Members;
- 10 b. Whether Defendant Amazon collected the biometric identifiers and
11 information of Plaintiffs and Class Members;
- 12 c. Whether Defendant Amazon stored the biometric identifiers and
13 information of Plaintiffs and Class Members;
- 14 d. Whether Defendant Amazon used the biometric identifiers and
15 information of Plaintiffs and Class Members;
- 16 e. Whether Defendant Amazon possessed the biometric identifiers and
17 information of Plaintiffs and Class Members;
- 18 f. Whether Defendant Amazon profited from the biometric identifiers and
19 information of Plaintiffs and Class Members;
- 20 g. Whether Defendant Amazon provided the notice required by BIPA
21 before obtaining the biometric identifiers and information of Plaintiffs
22 and Class Members;
- 23 h. Whether Defendant Amazon obtained written releases from Plaintiffs and
24 Class Members or their legally authorized representatives before
25

1 collecting, obtaining, storing and using the biometric identifiers and
 2 information of Plaintiffs and Class Members;

3 i. Whether Defendant Amazon had in place – and disclosed to the public –
 4 the written retention and destruction policies required by BIPA while in
 5 possession of Plaintiffs' and Class Members' biometric identifiers and
 6 information;

7 j. Whether Plaintiffs and Class Members suffered damages as a proximate
 8 result of Defendant Amazon's unlawful conduct; and

9 k. Whether Plaintiffs and Class Members are entitled to damages, equitable
 10 relief and other relief.

11 94. **Typicality.** Plaintiffs' claims are typical of the claims of the Class they seek to
 12 represent because Plaintiffs and all members of the proposed Class have suffered similar
 13 injuries as a result of the same practices alleged herein. Plaintiffs have no interests to advance
 14 adverse to the interests of the other members of the proposed Class.

15 95. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the
 16 proposed Class and have retained as their counsel attorneys experienced in class actions and
 17 complex litigation.

18 96. **Superiority.** A class action is superior to other available means for the fair and
 19 efficient adjudication of this dispute. The injury suffered by each Class Member, while
 20 meaningful on an individual basis, may not be of such magnitude as to make the prosecution of
 21 individual actions against Defendant Amazon economically feasible. Even if Class Members
 22 could afford individual litigation, those actions would put immeasurable strain on the court
 23 system. Moreover, individual litigation of the legal and factual issues of the case would increase
 24 the cost of justice to the parties and the public.

1 the delay and expense to all parties and the court system. A class action, however, presents far
2 fewer management difficulties and provides the benefit of a single adjudication, economy of
3 scale and comprehensive supervision by a single court.
4

5 97. In the alternative, the proposed Class may be certified because:

6 a. The prosecution of separate actions by each individual member of the
7 proposed Class would create a risk of inconsistent adjudications, which
8 could establish incompatible standards of conduct for Defendant
9 Amazon;

10 b. The prosecution of individual actions could result in adjudications that as
11 a practical matter would be dispositive of the interests of non-party Class
12 Members or which would substantially impair their ability to protect their
13 interests; and

14 c. Defendant Amazon acted or refused to act on grounds generally
15 applicable to the proposed Class, thereby making final and injunctive
16 relief appropriate with respect to members of the proposed Class.
17

18 98. Pursuant to Rule 23(c)(4), particular issues are appropriate for certification –
19 namely the issues described in paragraph 93, above – because resolution of such issues would
20 advance the disposition of the matter and the parties' interests therein.
21

CLAIMS FOR RELIEF

COUNT ONE
(VIOLATION OF BIPA – 740 ILCS § 14/15(b))

99. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as though fully set forth herein.

100. As alleged above, Defendant Amazon violated BIPA by collecting and obtaining individuals' biometric identifiers and information, including the biometric identifiers and information of Plaintiffs and Class Members, without providing the requisite written information and without obtaining the requisite written releases.

101. Defendant Amazon's violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

102. As a direct and proximate result of Defendant Amazon's violations of BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

103. Plaintiffs and Class Members seek as monetary relief the greater of \$5,000 or actual damages or, pleaded in the alternative, \$1,000 or actual damages.

104. Unless and until enjoined and restrained by order of this Court, Defendant Amazon's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and Class Members' biometric identifiers and information.

105. Plaintiffs and Class Members also seek punitive damages, injunctive relief and the reasonable attorney's fees, costs and expenses relating to this action.

COUNT TWO
(VIOLATION OF BIPA – 740 ILCS § 14/15(c))

106. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint, as though fully set forth herein.

107. As alleged above, Defendant Amazon violated BIPA by unlawfully profiting from individuals' biometric identifiers and biometric information, including the biometric identifiers and information of Plaintiffs and Class Members.

108. Defendant Amazon's violations of BIPA were intentional and reckless or, pleaded in the alternative, negligent.

109. As a direct and proximate result of Defendant Amazon's violations of BIPA, Plaintiffs and Class Members have suffered and will continue to suffer injury.

110. Plaintiffs and Class Members seek as monetary relief the greater of \$5,000 or
actual damages or, pleaded in the alternative, \$1,000 or actual damages.

111. Unless and until enjoined and restrained by order of this Court, Defendant Amazon's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that their biometric identifiers and information can be viewed and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for their injuries in that a judgment for monetary damages will not end the misuse of Plaintiffs' and Class Members' biometric identifiers and information.

112. Plaintiffs and Class Members also seek punitive damages, injunctive relief and the reasonable attorney's fees, costs and expenses relating to this action.

COUNT THREE
(UNJUST ENRICHMENT)

113. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as though fully set forth herein.

114. Defendant Amazon obtained a monetary benefit from Plaintiffs and Class Members to their detriment. Defendant did so by profiting off of Plaintiffs' and Class Members' biometric identifiers and information, while exposing Plaintiffs and Class Members to a heightened risk of privacy and informational harms and depriving them of their control over their biometric data.

115. Plaintiffs and Class Members did not authorize Defendant Amazon to collect, obtain, store, use, possess and profit off of their biometric identifiers and information.

116. Defendant Amazon appreciated, accepted and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Defendant's conduct toward Plaintiffs and Class Members as described herein.

117. Defendant Amazon profited from Plaintiffs' and Class Members' biometric identifiers and information and did not provide full compensation for the benefit received from Plaintiffs and Class Members.

118. Defendant Amazon obtained Plaintiffs' and Class Members' biometric identifiers and information through inequitable means in that it obtained biometric data from Plaintiffs' and Class Members' online photographs without permission and in violation of Illinois law.

119. Plaintiffs and Class Members have no adequate remedy at law.

120. Under the circumstances, it would be unjust and unfair for Defendant Amazon to be permitted to retain any of the benefits obtained from Plaintiffs and Class Members and their biometric identifiers and information.

121. Under the principles of equity and good conscience, Defendant Amazon should not be permitted to retain the biometric identifiers and information belonging to Plaintiffs and Class Members because Defendant unlawfully obtained the biometric identifiers and information.

122. Defendant Amazon should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received as a result of obtaining, collecting, storing, using, possessing and profiting off of Plaintiffs' and Class Members' biometric identifiers and information, including but not limited to the value of the intellectual property derived therefrom.

COUNT FOUR

INJUNCTIVE RELIEF

123. Plaintiffs restate and reallege all paragraphs of this Class Action Complaint as though fully set forth herein.

124. Plaintiffs and Class Members have clear and ascertainable rights in need of protection – namely: (a) the right to have Defendant Amazon abide by its obligations under BIPA; (b) the right to control their biometric identifiers and information; and (c) the right to privacy.

125. Plaintiffs and Class Members have no adequate remedy at law because a legal remedy cannot retrieve the biometric identifiers and information that Defendant Amazon unlawfully collected, obtained, stored, used, possessed and otherwise profited from, and cannot end the invasion of privacy caused by Defendant's conduct.

126. Plaintiffs and Class Members will suffer irreparable harm, as alleged herein, caused by Defendant Amazon if its conduct is not so restrained, requiring injunctive relief.

127. Plaintiffs and Class Members are likely to succeed on the merits because, as alleged herein, Defendant Amazon unlawfully collected, obtained, stored, used, possessed and otherwise profited from Plaintiffs' and Class Members' biometric identifiers and information despite being prohibited from doing so.

128. Plaintiffs and Class Members seek injunctive relief: (a) barring Defendant Amazon from any further use of Plaintiffs' and Class Members' biometric identifiers and information; (b) barring Defendant Amazon from continuing to collect, obtain, store, use, possess or profit from Plaintiffs' and Class Members' biometric identifiers and information; and (c) requiring Defendant Amazon to delete and destroy Plaintiffs' and Class Members' biometric identifiers and information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Steven Vance and Tim Janecyk, on behalf of themselves and on behalf of the Class, respectfully seek from the Court the following relief:

- a. Certification of the Class as requested herein;
- b. Appointment of Plaintiffs as Class representatives and their undersigned counsel as Class counsel;
- c. An award of damages for Plaintiffs and members of the proposed Class, including statutory and punitive damages;
- d. An award of equitable, injunctive and declaratory relief for Plaintiffs and members of the proposed Class, including an injunction (i) barring Defendant Amazon from any further use of the biometric identifiers and information of Plaintiffs and members of the Class; (ii) barring Defendant from continuing to collect, obtain, store, use, possess and profit from

1 biometric identifiers and information of Plaintiffs and members of the
2 Class; and (iii) requiring Defendant to delete and destroy all biometric
3 identifiers and information of Plaintiffs and members of the Class;

4

5 e. An order requiring Defendant Amazon to disgorge into a common fund
6 or constructive fund, for the benefit of Plaintiffs and members of the
7 proposed Class, proceeds that it unjustly received as a result of its
8 collection, obtainment, storage, use, possession and profiting off of
9 Plaintiffs' and Class Members' biometric identifiers and information;

10

11 f. An award of pre-judgment and post-judgment interest for Plaintiffs and
12 members of the proposed Class, as permitted by law;

13

14 g. An award for Plaintiffs and members of the proposed Class of reasonable
15 attorneys' fees and costs of suit, including expert witness fees; and

16

17 h. An award for Plaintiffs and members of the proposed Class of any further
18 relief the Court deems proper.

JURY DEMAND

Plaintiffs hereby demand a trial by jury pursuant to Federal Rule of Civil Procedure 38(b) on all issues so triable.

Dated this 14th day of July, 2020

STEVEN VANCE and TIMOTHY JANECYK, for
themselves and others similarly situated,

By:

David B. Owens, WSBA #53856
Attorney for Plaintiffs

David B. Owens
LOEJVY & LOEJVY
100 S. King Street, Suite 100
Seattle, WA 98104
david@loevy.com

Michael Kanovitz*
Scott R. Drury*
LOEJVY & LOEJVY
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900
mike@loevy.com
drury@loevy.com

* *pro hac vice* applications forthcoming

Gary Lynch*
Katrina Carroll*
Kyle A. Shamberg*
Nicholas R. Lange*
CARLSON LYNCH LLP
111 West Washington Street, Suite 1240
Chicago, Illinois 60602
312.750.1265
glynch@carlsonlynch.com
kcarroll@carlsonlynch.com
kshamberg@carlsonlynch.com
nlange@carlsonlynch.com

* *pro hac vice* applications forthcoming